DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Enterprise Commercial Solutions for Classified (CSfC) Gateway Convergence "Universal DoDIN Gateway"

Mr. J Tracy Allison
Communications Gateway Division
May 16, 2019

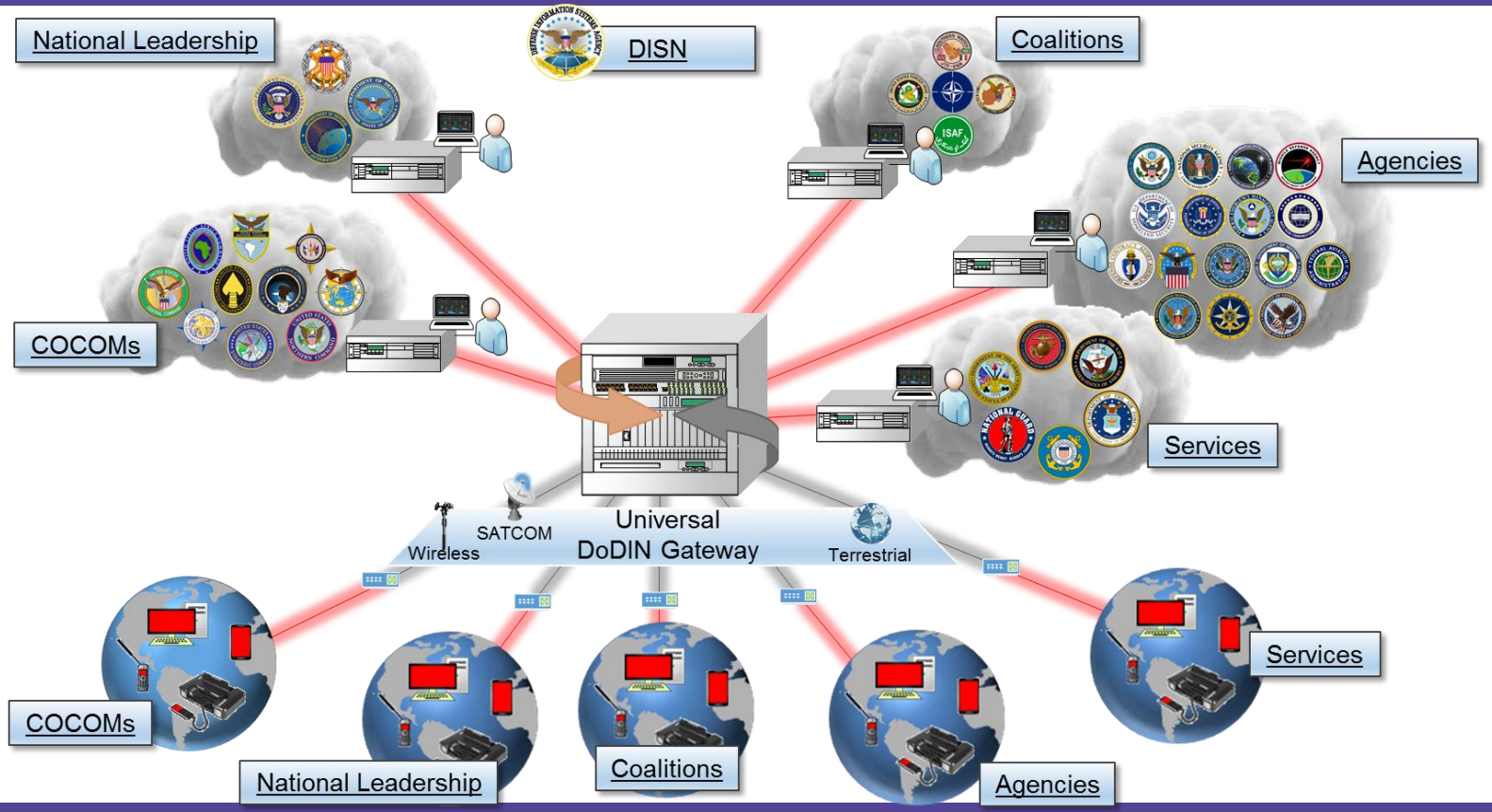
Universal DoDIN Gateway

- **The Universal Gateway will consist of all enterprise infrastructure required to support terrestrial, mobile and satellite communications services (voice, video and data) to all DoDIN customers worldwide.**

- **Numerous, existing discrete gateways (e.g. DMCC, DECTK, etc) will be converged into a single gateway architecture incorporating new Commercial Solutions for Classified (CSfC) capabilities while continuing to support traditional encryption methods using Type 1 hardware.**

- **The Universal Gateway will provide all required gateway functions at all layers of the OSI stack for all communications entering or exiting the DoDIN regardless of whose it is or what it is or where it is going or how it is getting there.**

Universal DoDIN Gateway Vision



Road to Universal DoDIN Gateway

- **Commercial Solutions for Classified (CSfC) is used in several existing DISA-provided systems and represents the future of encryption for everyday classified mobile and transportable communications.**
- **Numerous mission partners have expressed a desire to migrate to a DISA-provided Enterprise CSfC System versus continuing to sustain their own gateways.**
- **DISA's goal is to fully support emerging CSfC capabilities as well as traditional encryption methods via all transport mechanisms.**

Road to Universal Gateway (continued)

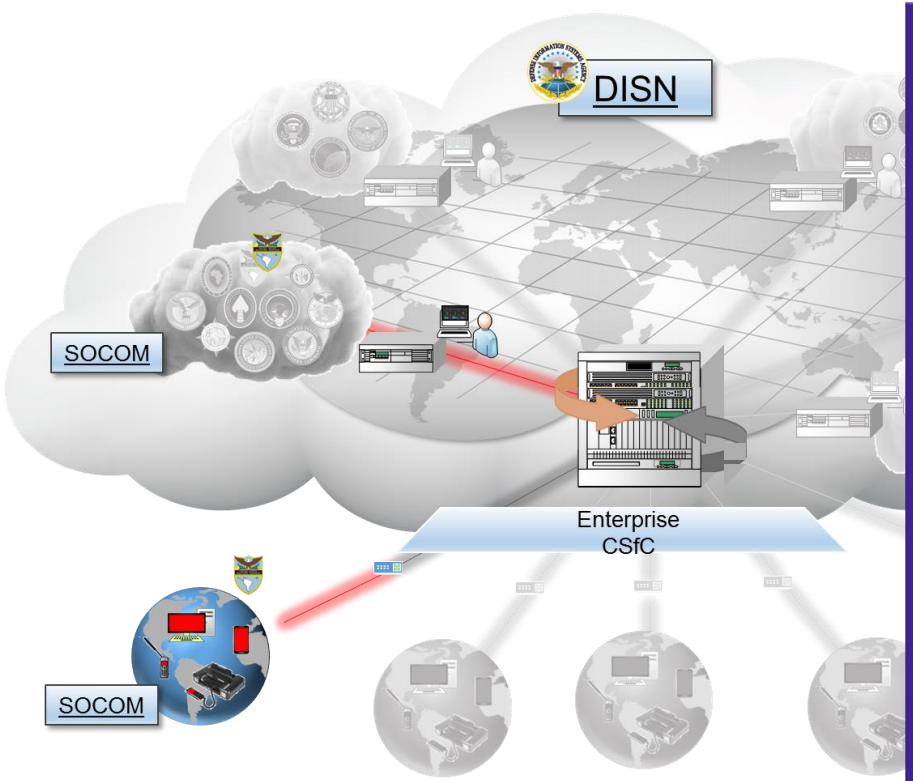
- **CSfC requires more system-level approvals than traditional security mechanisms, so we are currently focused on CSfC-specific requirements in order to implement a sound architectural solution.**
- **DISA is currently converging several discrete gateways and will field the first consolidated system later this year.**
- **Decisions on COAs to achieve the Universal Gateway will be made 4QFY19**

Enterprise CSfC General Definition

Enterprise CSfC will allow mission partners greater connectivity to classified networks by using commercial-grade encryption technology to securely traverse any unclassified, internet, or non-DoD network.

- ✓ **Customers use commercial internet to access the DISN for common services and their own classified enclaves for mission specific activities**
- ✓ **Access classified data without Type 1 Encryption hardware (or classified device)**
- ✓ **Support multiple customer devices (travel kits, smartphones, tablets, etc.)**
- ✓ **Design for regular introduction of new devices (keep up with innovation)**
- ✓ **Vendor agnostic**
- ✓ **DISA-provided Enterprise DOD PKI Certificate Management System**
- ✓ **DISA-provided "Shared" Enterprise Management Systems (e.g. Network, Cyber, etc.)**
- ✓ **Comply with approved NSA Capability Packages (eventually support Global Gray)**
- ✓ **Future potential for Multi-Domain, Single Device**

Enterprise CSfC Organization Control

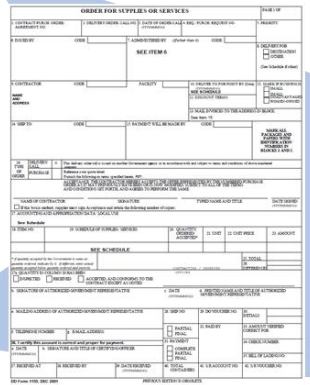


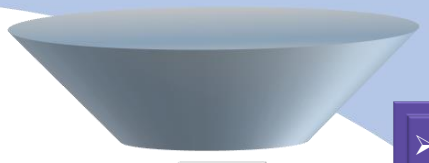
Features

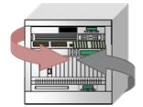
- ✓ Enterprise PKI Certificate Management System
  - ✓ Provides management for ALL certificates
  - ✓ Request, Create, Distribute and Revoke
  - ✓ Customer manages own certificates
  - ✓ DISA provided system
- ✓ Enterprise “Shared Access” Management Systems
  - ✓ All required Enterprise Management Functions
  - ✓ Common Awareness
  - ✓ Improved Efficiency and Effectiveness
  - ✓ Shared responsibility
- ✓ Flexible device support (multiple options)
  - ✓ Turn key (APL devices pre-approved)
  - ✓ Custom (DISA-assisted approval)
- ✓ Converges multiple existing capabilities
- ✓ Potential multi-domain single device (future)

Enterprise CSfC

- Leverage existing DoD CSfC efforts
  - DMCC, DECTK, JCSE, etc.
  - TRL 8 (No R&D)
  - Build on Foundation
- FGGM DISA lab to host development
- Converge Systems to Single Gateway
- Build Prototype
- Deploy Initial Converged Capability







- Refine requirements with Stakeholders
  - COI WG Distribution (growing)
  - DoD (JSAP)
  - Industry (RFI / Industry Day)
- Rapid Acquisition Approach
  - Incentive Contract / OTA?
  - NSA Trusted Integrator
- Continue to work foundation projects

- Production for Enterprise Deployment
- Incentivized contracts for speed/capability
- Enterprise Management Systems
- Full O&M Support Structure
- Capacity Services-Based (to extent possible)
- Flexible Device Access (APL and Custom)

CSfC Converged Gateway (C2G) IPT

C2G-IPT is established to design and build a (prototype) converged gateway based on current CSfC standards in 90 days. The goal is to demonstrate gateway is capable of supporting existing CSfC DECTK-GW and DMCC-S end user devices and capabilities.

Outcomes:

- **At least 3 Architectural Courses of Action (COA's) for gateway convergence**
- **Solution Architecture**
  - **NSA & CEP (Chief Engineers Panel) Review**
  - **Prototype CSfC Gateway & Demonstration**
- **Publish results that inform future investments**

DoD Mobility Classified Capability – Secret (DMCC-S)

DoD Mobility Classified Capability - Secret (DMCC-S) is an enterprise service that enables government owned Mobile Devices access to the Classified Secret Department of Defense Information Network (DoDIN) telephony and information services. DMCC-S is configured to the National Security Agency's (NSA) Commercial Solutions for Classified (CSfC) Mobile Access Capability Package (MACP). Since the Custom Read Only Memory (CROM) DMCC-S phone and tablet devices contain no data-at-rest, they are considered unclassified when powered off. Mission Partners are required to log into their DMCC-S device and their Secret Internet Protocol Router (SIPR) account via a hard-wired SIPR station every 30 days to ensure account activity and device update.

DECTK-GW System Descriptions

- **DoD Enterprise Classified Travel Kit - Gateway (DECTK-GW)** is a Secret IP Network (SIPRNet) extension capability that will provide Combatant Commanders, other high-profile users and Warfighters remote access via the internet to Enterprise Classified Voice over Internet Protocol (ECVoIP) and SIPERNet data services.

- **Non DoD Enterprise Classified Travel Kit - Gateway (NonDECTK-GW)** enables secure voice communications between the U. S. DoD leadership and their counterparts in other nations using a VoIP end instrument as part of a deployable end-point with foreign releasable encryption devices and foreign releasable key material to protect these communications.

- **Commercial Solutions for Classified (CSfC) for DoD Enterprise Classified Travel Kit – Gateway (DECTK-GW)** – CSfC is a set of commercial products used in layered solutions to manage and protect classified National Security System (NSS) information. DECTK has a limited CSfC capability which allows mission partners to communicate securely at the SECRET level from anywhere without hardware encryptors.

Summary

- **Adhere to approved NSA capability standards for CSfC**
- **Continue to gather and refine customer requirements**
- **Complete C2G Prototype (3QFY19)**
- **Determine Way Ahead based on output of C2G IPT (3/4QFY19)**
- **Converge CSfC (C2G) and Traditional encryption capabilities (4QFY19)**
- **Modify pre-production prototype for deployment (4QFY19) adding monitoring, failover, etc.**
- **Develop Convergence Plan (4QFY19) for phased development/deployment (Service labs, etc)**
- **Deploy initial phase Universal Converged Gateway capability (1QFY20)**
- **Execute plan to converge gateway functions to create Universal DoDIN Gateway (start 1QFY20)**

QUESTIONS?

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**

visit us

DISA Booth 1929

follow us

Facebook/USDISA

Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at **www.disa.mil/about/industry-partners**.